**Integrated Funds, Distribution,
Control Point Activity, Accounting
And Procurement (IFCAP)**

PACKAGE SECURITY GUIDE

"SENSITIVE INFORMATION"

Version 5.1
October 2000

Department of Veterans Affairs
VIST**A** Technical Services

Preface

Purpose of the Security Guide

The Security Guide specifies parameters controlling the release of sensitive information related to the Integrated Funds Distribution, Control Point Activity, Accounting and Procurement (IFCAP) V. 5.1 software.

This document will be excluded from any Freedom of Information Act (FOIA) request releases. Distribution of this document is restricted to the Information Resource Management (IRM) Service and ADP Security Officer (ADPSO). Since certain keys and authorizations must be delegated for proper management of the system, information about these items may be found elsewhere in the technical and user manuals.

Reference Numbering System

This document uses a numbering system to organize its topics into sections and show the reader how these topics relate to each other. For example, section 1.3 means this is the main topic for the third section of Chapter 1. If there were two subsections to this topic, they would be numbered 1.3.1 and 1.3.2. A section numbered 2.3.5.4.7 would be the seventh subsection of the fourth subsection of the fifth subsection of the third topic of Chapter 2. This numbering system tool allows the reader to more easily follow the logic of sections that contain several subsections.

Table Of Contents

Chapter 1 Introduction

1.1 Security Management - Restrictions for Using Fiscal and Procurement Data

The IFCAP (Integrated Funds Distribution, Control Point Activity, Accounting, and Procurement) V. 5.1 package deals with the activities and data related to the fiscal and procurement processes at your facility. The need for package security is addressed throughout this software, affording every effort to restrict the mishandling of IFCAP functionality. A significant amount of testing, as well as VA Central Office review, has been conducted on the entire IFCAP package. The Office of Acquisition and Materiel Management (OA&MM), and the Office of Budget and Finance, have requested that each facility utilizing the IFCAP package appreciate the sensitivity of these issues. It is for these reasons that each facility is reminded that ***local modification of program code is expressly prohibited.***

1.2 Modifying Routines

The modification of IFCAP V. 5.1 routines is covered by the Veterans Health Administration (VHA) Manual, M-11, "Information Resources Management", Chapter 9, "Software Management". The complete text may be found at http://vista.med.va.gov/policies/m-11ch9.doc. A portion is quoted below:

9.11 PROCEDURES FOR SITE IMPLEMENTATION

b. Local Modification of Software

(1)   Where a national package implements a controlled procedure (e.g., payroll processing, procurement, fee basis, medical quality control) which in turn reports data to a data base outside the VHA environment (e.g., CALM, Automated Medical Information System (AMIS)), there must be no alteration of that package except by the Development ISC. National package routines relating to security features or fiscal integrity also must not be altered except by the Development ISC.
…

(5)   Local modifications of national package routines are strongly discouraged.   If local modifications are made to existing routines in national packages it will then be the responsibility of the modifying health care facility to maintain those modifications.

1.3 Modifying Data Dictionaries

The modification of IFCAP V. 5.1 data dictionaries is covered by the Veterans Health Administration (VHA) Manual, M-11, "Information Resources Management," Chapter 4, "Data Base Administration." The complete text may be found at http://vista.med.va.gov/policies/m-11ch4.doc. A portion is quoted below:

4.07 PROCEDURES FOR MODIFICATIONS TO DATA DICTIONARIES

a. Modifications to national package data dictionaries should be restricted to the addition of new data elements and to the creation of input and output templates to meet specific needs of local sites. To ensure the capability of installing new releases of the application packages, it is important that any local additions to the data base be made in areas that will not conflict with elements contained in the nationally distributed data base.

b. When adding new data elements to the VA FileMan data dictionary, the numbering conventions used for creating new files should also be used for data elements.

(1) A data element number should be entered that is in the numbering range of the assigned numbering prefix multiplied by 1000.

(2) The same convention should be applied to global subscripts for local data add-ons to previously defined globals.

c. The VA FileMan subdictionary numbers should be assigned at the high end of the numbering sequence, following the numbering convention outlined. For example, a VA FileMan subdictionary number added to the Patient file (File 2) by station 368 should be 2.368001, a second subdictionary should be assigned 2.368002, and so forth.

d. The VA FileMan data dictionary may be modified only through tools provided by the VA FileMan or by tools specifically referenced in the VA FileMan Programmer's Manual.

e. To keep conflicts with cross-references to a minimum, field facilities creating custom cross-references must use the number range assigned to the site and prefix with "AZ" or "Z".

(1) National packages are not permitted to use these cross-references.

(2) Cross-reference numbers should be assigned based on the station number multiplied by 1000.

f. All other types of local data modifications to national packages are strongly discouraged. If local modifications are made to existing data elements in a national package data dictionary, it will then be the responsibility of the site to maintain those modifications as new versions of the package are installed.

g. When software components are incorporated into the package, the names associated with the new components (e.g., routines, options, templates) should be prefixed by the package namespace followed by the letter "Z".

(1) For example, a local option called "LOG" for the PSIV package would have the option name "PSIVZLOG".

(2)   Prefixing allows the site to readily differentiate between components developed locally and those associated with the DHCP national packages.

(3)   Namespaces of one, two, three, or four characters followed by "Z*" shall not be exported in nationally developed software, but shall be reserved for local use.

1.4 Menu Assignments

The concern for package security includes the menus assigned to the IFCAP user. *NO IFCAP USER should have access to all of the options available.* Just as a Control Point Official should not have the ability to enter a Ceiling Transaction, neither should a Purchase Agent be able to obligate a Purchase Order. The standardized menus that accompany this package were specifically designed to account for those functions that are performed in Fiscal, A&MM, and Control Points. Although you have the ability to customize menus for a user, be aware of potential conflicts of interest. Be careful not to circumvent the checks and balances required in your daily operations.

(This page intentionally left blank.)

Chapter 2 Electronic Signature

2.1 Overview

A primary aspect of security in IFCAP involves the use of **Electronic Signatures**. Individuals in the system who have authority to approve actions, at whatever level, have the ability to enter and edit their own Electronic Signature Code. This code is required before the documents pass on to a new level for processing or review. Like the access and verify codes used when gaining access to the system, the Electronic Signature Code will not be visible on the terminal screen. These codes are also encrypted so that even when viewed in the user file by those with the highest levels of access, they are unreadable. Electronic Signature codes are required by IFCAP at every level that currently requires a Signature on paper. Electronic Signature codes are required for: Budget Analysts distributing funds to Control Points; Control Point Officials (not Control Point Clerks or Initiators) approving requests; Purchasing Agents processing purchase orders; Accounting Technicians obligating documents; Voucher Auditors authorizing payments; and Warehouse personnel receiving purchases.

Those individuals with Electronic Signature Codes have a menu option, located on their secondary menu (User's Tool Box) that allows them to change their Signature Code at any time.

2.2 Required Electronic Signatures

- Accountable Officer   Process Requests in PPM & Federal Requisition Orders
- Budget Analyst   Release Funds to Control Points
- Control Point Official   Approve Requests
- Purchasing Agent   Sign Purchase Orders
- Accounting Technician   Obligate Documents
- Voucher Auditors   Certifying Payments
- Warehouse Workers   Receiving Reports
- Requisition Clerk   Requisition Processing and Code Sheet
- Requirements Analyst   Requisition Processing and Code Sheet

2.3 Electronic Signature Design

An Electronic Signature is designed as a two-part process and is described in the following section.

2.3.1   Identification

Identification (or "hashing") is system verification that the person who logged in is the same person accessing a document. This process of identification uses the Electronic Signature (ESIG) Code string, which it passes through a hashing algorithm and compares it to a string maintained in the user file of the person currently logged into the system. A match indicates (unless a user has "shared" his/her ESIG Code with another person) that the person entering the ESIG Code is the "logged-in" user. The identification process can and is used independently of the record authentication function.

2.3.2   Authentication

Authentication (or "encoding") marks an electronic record within the **V***IST***A** with the identification of the user. This process takes the internal record number of the record being secured (i.e., the Signature Block Name of the person signing the record and that person's internal record number in the NEW PERSON file # 200) and passes it through a second algorithm to create a string. "Decoding" of the string occurs as the reverse of the process just described. The matching of the user Signature Block Name and the outcome of the Decoding process validates that the Electronic Signature is "tamper free".

Chapter 3 IFCAP Security Keys & Other Features

3.1 Description of Security Keys

This list of security keys is also found in chapter 5 of the IFCAP V. 5.1 Technical Manual.

PRCFA PURGE CODE SHEETS
DESCRIPTION: This key is required to use the purge old code sheets from the system.
   (NO OPTIONS)

PRCFA SUPERVISOR
KEEP AT TERMINATE: YES
DESCRIPTION: This key must be assigned to the Accounting Supervisor. It locks the following options:
   Purge Transmission Records/Code Sheets [PRC GECS PURGE]
   Retransmit Stack File Document [PRC GECS STACK RETRANSMIT]
   Enter/Edit Date When SOs become ARs [PRC SO TO AR]
   Audit Reports Menu [PRCF AUDIT REPORTS]
   Clear Program Lock [PRCFA CLEAR LOCK]
   Rebuild a Code Sheet Template [PRCFA REBUILD CODE SHEET MAP]
   Stacked Fiscal Documents Menu [PRCFA STACK DOCUMENTS]

PRCFA TRANSMIT
DESCRIPTION: This key is required to be held by any user authorized to release Receiving Report code sheet batches to Austin. This key locks the following options:
   Retransmit Code Sheets Batch to Austin [PRCFA RETRANSMIT BATCH]
   Transmit Receiving Reports on Transmission List [PRCFA RR TRANSMIT]
   Transmit Code Sheets to Austin [PRCFA TRANSMIT CODE SHEETS]

PRCFA VENDOR EDIT
DESCRIPTIVE NAME: PRCFA VENDOR EDIT FMS FIELDS
DESCRIPTION: This security key provides access to edit certain critical fields like the FMS Vendor ID and the Alternate-Address Indicator, which are normally populated by incoming transactions sent by FMS. This key locks the following options:
   Setup AR selected vendors [PRCO AR VENDOR EDIT]
   Review VENDOR REQUEST [PRCO VRQ REVIEW]

PRCH AR
DESCRIPTIVE NAME: APPROVE RECONCILED ORDER
DESCRIPTION: This is a key to lock the Approving Official Menu [PRCH APPROVE] option.

PRCH TRANSACTION COMPLETE
DESCRIPTIVE NAME: All Status Amendment Key
DESCRIPTION: The holder of this key will be able to amend a PO or Requisition even if the Status is Transaction Complete. This key locks the following options:
    All Status Amendment to PO [PRCH ALL STATUS AMEND TO PO]
    All Status Amendment to Req [PRCH ALL STATUS AMEND TO REQ]

PRCHADVOUCHER
DESCRIPTION: The holder of this key can create adjustment vouchers for receiving reports and requisitions. It is recommended that this key be assigned to the chief of P & C. This key locks the following options:
    Adjustment Voucher to Receiving Report [PRCH ADJUSTMENT VOUCHER]
    Adjustment Voucher to Requisition [PRCHPM REQN ADJ VOUCHER]

PRCHASSIGN
DESCRIPTION: Allows holder to assign 2237 request to a specific purchasing agent. This key locks the following option:
    Assign a Request to Purchasing Agent [PRCHPC ASSIGN REQUEST]

PRCHIMP
DESCRIPTION: This key allows the holder access to the main menu for processing Imprest Funds type Purchase Orders. This key locks the following menu:
    Imprest Funds Processing Menu [PRCHPC IMPREST FUND MENU]

PRCHPM CS PURGE CODE SHEETS
DESCRIPTION: Key allowing user to purge LOG, GSA or DLA code sheets from LOG Code Sheet File. This key locks the following option:
    Purge Code Sheets (LOG/GSA/DLA) [PRCHPM CS PURGE]

PRCHPM CS TRANSMIT
DESCRIPTION: Key allowing holder to transmit LOG, GSA or DLA code sheets to Austin or DLA. This key locks the following options:
    Add Code Sheet to Printed Batch (LOG/GSA/DLA) [PRCHPM CS ADD TO BATCH]
    Delete Code Sheet from Printed Batch (LOG/GSA/DLA) [PRCHPM CS DELETE FROM BATCH]
    Re-transmit Batch to Austin (LOG/GSA/DLA) [PRCHPM CS RE-TRANSMIT BATCH]
    Transmit Code Sheets to Austin (LOG/GSA/DLA) [PRCHPM CS TRANSMIT]

PRCHRECDEL
DESCRIPTION: This key allows its holders to delete a Receiving Report for a purchase order. This key locks the following option:
    Delete a Receiving Report [PRCHPM PO DEL REC]

PRCHRPT
DESCRIPTION: The holder is allowed to use the reprint menu of the management report menu.
This key locks the following menu:
    Reprints Menu [PRCHOUT REPRINT]

PRCP MGRKEY
DESCRIPTION: This key unlocks the PRCP MANAGER MENU (Primary Inventory)

PRCP2 MGRKEY
DESCRIPTION: This key unlocks the PRCP2 MANAGER MENU (Secondary Inventory)

PRCPW ADJAPPR
DESCRIPTION: This key is used to lock the Approve Adjustments [PRCPW ADJUST
APPROVAL] menu.

PRCPW MGRKEY
DESCRIPTION: This key unlocks the PRCPW MANAGER MENU (Warehouse Inventory)

PRCSCPO
KEEP AT TERMINATE: YES
DESCRIPTION: This key is for the Control Point Official. This key locks the following
options:
    Approve Requests [PRCSAPP]
    Enter/Edit Control Point Users [PRCSCPU]
    Enter FCP Adjustment Data [PRCSENA]

PRCSOBL
DESCRIPTION: This key is used to restrict access to the 'Obligation Data' option. It may be
assigned to A&MM personnel who perform issue book processing, to Fiscal personnel, and to
control point officials and clerks. This key locks the following option:
    Obligation Data [PRCSENOD]

PRCT MGR
DESCRIPTION: This key restricts the ability to modify barcode programs and parameters that
will affect the operation of barcode programs. This key should only be given to IRM service
personnel. This key locks the following menu:
    Programmer (Barcode) Menu [PRCT PROGRAMMER (BARCODE)]

3.2 Mail Groups

A listing and description of Mail Groups appears in chapter 6 of the IFCAP V. 5.1 Technical Manual.

3.3 Bulletins

A listing and descriptions of Bulletins appears in chapter 6 of the IFCAP V. 5.1 Technical Manual.

3.4 Archiving/Purging

A description of the archiving and purging processes appears in chapter 7 of the IFCAP V. 5.1 Technical Manual.

3.5 Contingency Planning

Using services must develop a local contingency plan to be used in the event of product problems in a live environment. The facility contingency plan must identify the procedure for maintaining the functionality provided by IFCAP V. 5.1 in the event of system outage. Field station ISOs may obtain assistance from their Regional Information Security Officer (RISO).

3.6 Interfacing

There are two bar-code readers utilized within VA Medical Centers:
- Intermec 9440 readers
- Janus 2020 bar-code readers

3.7 References

The following handbooks contain materials that related to IFCAP V. 5.1:
- FMS Handbook
- VHA Handbook 4671.1 - Cost Centers
- VHA Handbook 4671.2 - Budget Object Codes (Draft)
- VHA Handbook 1730.1 - Use and Management of the Government Purchase Card Program

3.8 Remote Systems

The following entries describe the data transmitted from IFCAP V. 5.1 to remote system/facility databases.

3.8.1. EDI Transactions

Electronic Request for Quotations (X12 840 transaction), Text Message (X12 864 transaction) and Purchase Order (X12 850 transaction) are sent in MailMan e-mail messages from IFCAP systems to the EDI group of OA&MM in Austin, TX. The TCP/IP handles accuracy within the mail transmission. Upon receipt, the receiving mail system sends back a Confirmation Message listing the Identification Number of the message on that mail system and an assigned Confirmation Number. When the transactions are processed by the EDI group's software, an 'ACT' transaction is send to the submitting station if the message could be properly processed, while a 'PRJ' message is sent if there was a problem with the format or content of the transaction. In EDI Purchase Orders whose method of payment is Purchase Card, a VA specific algorithm encrypts the Card Number and Expiration Date fields. The code implementing the encoding, like the rest of IFCAP, is not available under the Freedom of Information Act. With EDI Purchase Orders, a vendor responding to the order may send back a Purchase Order Acknowledgement transaction (X12 855 transaction) indicating acceptance of the order and providing updates to delivery schedule, pricing and quantity or indicating rejection of the order. The receipt of a POA indicates that the order successfully arrived at the vendor.

3.8.2 Procurement History Transactions

When items are ordered, IFCAP sends a Procurement History Activity (PHA) transaction in a MailMan e-mail message to a centralized, OA&MM procurement history database in Austin, TX. This contains information on the vendor supplying the goods, description of the goods and pricing. When amendments are done to the order, a Procurement History Modification (PHM) transaction is sent to this database. The TCP/IP handles accuracy within the mail transmission. Upon receipt, the receiving mail system sends back a Confirmation Message listing the Identification Number of the message on that mail system and an assigned Confirmation Number.

3.8.3 LOG Transactions

IFCAP sends information related to changes in quantities of items in the Supply Fund warehouse inventories and related to orders from federal vendors in LOG code sheets, which are packed into MailMan e-mail messages and sent to an Austin TX OA&MM database.   The TCP/IP handles accuracy within the mail transmission. Upon receipt, the receiving mail system sends back a Confirmation Message listing the Identification Number of the message on that mail system and an assigned Confirmation Number.

3.8.4 Financial Transactions to the Financial Management System (FMS) in Austin, TX

IFCAP sets up documents describing the distribution of funds, financial data on obligations for goods and services, invoice amounts from receipt of goods and services, and requests for transfer of funds between accounts. IFCAP also sends Vendor Request transactions (VRQs) to add new vendors to the FMS vendor database and to request updates to the IFCAP database with the FMS vendor IDs, alternate address indicators, and payment addresses. These documents are handed off to the VISTA Generic Code Sheet module. This module then loads the documents into MailMan e-mail messages sent to the Financial Services Center in Austin, TX. The frequency that the Generic Code Sheet processes batched documents is site configurable, with 'every 15 minutes' being a common value. Documents can have a future transmission date specified so that they are held for later transmission. The TCP/IP handles accuracy within the mail transmission. Upon processing these transactions, the FMS sends a Document Confirmation Transaction (DCT) back to the sending station for updating the status of the record in the Generic Code Sheet Stack file, as accepted or rejected.

3.8.5 Receiving Reports

Upon the receipt of goods, IFCAP sends a RT transaction to IFCAP Receiving Report Program (IFRR) or Federal Receiving Report Program (INRR) for recording each receipt from a Non-Federal or Federal vendor, respectively. This transaction lists the total cost, cost by item, accounting information and vendor identification. The RT transaction is sent via a MailMan e- mail message to the IFRR/INRR database. The TCP/IP handles accuracy within the mail transmission. As with all MailMan messages send to other MailMan systems, the message transmission status and the Identification Number of the message in the receiving MailMan system is recorded in the copy at the originating site. Ultimately, receiver information is transferred to the Computer Assisted Payment Processing (CAPP) system, which after matching the receiver against a vendor's invoice generates the Receiving Report to be processed by FMS.

Chapter 4 File Protection and Security Access

4.1 File Protection

This file protection information is also found in chapter 4 of the IFCAP V. 5.1 Technical Manual.

The IFCAP V. 5.1 package files contain data that is prepared according to the policy and procedures of the Office of Budget and Finance and the Office of Acquisition and Materiel Management. Therefore, the files used by IFCAP generally carry a high level of file protection. The data dictionaries for IFCAP should NOT be altered. Screening logic has also been enabled on some IFCAP files to prevent access through VA FileMan.

The IFCAP package uses eight (8) VA FileMan file protection levels on its files:

>   None - where no special security is enabled
>   # - Site Manager access
>   @ - Programmer access to files
>   [- READ Access
>   ] - WRITE Access
>   % - Delete Access
> $ - LAYGO Access
>   ^ - Can not be accessed

4.2 Files and Security Access

This file security access information is also found in chapter 4 of the IFCAP V. 5.1 Technical Manual.

File Name	Number	DD Access	RD Access	WR Access	DEL Access	LAYGO Access
CONTROL POINT ACTIVITY	410	@	[	]	%	$
TRANSACTION NUMBER	410.1	@	[	]	%	$
CLASSIFICATION OF REQUEST	410.2	@	[	]	%	$
REPETITIVE ITEM LIST	410.3	@	[	]	%	$
SUB-CONTROL POINT	410.4	@	[	]	%	$
CPA FORM TYPE	410.5	@	[	]	%	$
DELIVERY SCHEDULE	410.6	@	[	]	%	$
SORT GROUP	410.7	@	[	]	%	
DELIVERY POINT	410.8	@	[	]	%	$
ADMIN. ACTIVITY SITE PARAMETE	411	@	[	]	%	$
FACILITY TYPE (TEMPORARY)	411.2	@	[	]	%	$
IFCAP CONVERSION DISCREPANCY	411.3					
IFCAP CONVERSION ERROR	411.4					
IFCAP PARAMETERS	411.5	@			%	
FMS TRANSACTIONS	417					
FMS EXCEPTIONS	417.1					

File Name	Number	DD Access	RD Access	WR Access	DEL Access	LAYGO Access
FUND CONTROL POINT	420	@	[	]	%	$
COST CENTER	420.1	@	[	]	%	$
PRCD SD PROGRAM	420.13					
PRCD SD FCP/PRJ	420.131					
PRCD SD OBJECT CLASS	420.132					
PRCD SD JOB	420.133					
PRCD SD REPORTING CATEGORY	420.134					
PRCD SD REVENUE SOURCE	420.135					
PRCD SD SUB-REV SOURCE	420.136					
PRCD SD SUB-OBJ	420.137					
PRCD SD FMS SECURITY	420.138					
PRCD FUND	420.14					
PRCD FMS SUB-ALLOWANCE ACCOUN	420.141					
PRCD SD ADMINISTRATIVE OFFICE	420.15					
PRCD SD DOCUMENT TYPE	420.16					
PRCD SD DOCUMENT DATA ELEMENT	420.17					
PRCD REQUIRED FIELDS	420.18					
PRCD STANDARD DICTIONARY	420.19					
PRCD SD STATUS	420.1999					
BUDGET OBJECT CODE	420.2	@	[	]	%	$
PRCD FUND/APPROPRIATION CODE	420.3	@	[	]	%	$
CALM/LOG TRANSACTIONS CODE LI	420.4	@	[	]	%	$
UNIT OF ISSUE	420.5	@	[	]	%	$
CODE INDEX	420.6	@	[	]	%	$
BUDGET DISTRIBUTION CODES	420.7	@	[	]	%	$
SOURCE CODE	420.8	@	[	]	%	$
INTERMEDIATE PRODUCT	420.9	@	[	]	%	$
PRCU IFCAP/FMS CONVERSION	420.92					
IFCAP/FMS OBLIGATION RECONCIL	420.96					
IFCAP/FMS FCP RECONCILIATION	420.97					
IFCAP/FMS FCP RECONCILIATION	420.98					
IFCAP TEMP FCP SNAPSHOT	420.99					
PRCD SD STANDARD FOR COPYING	420.9999					
FUND DISTRIBUTION	421	@	[	]	%	$
MULTIPLE DISTRIBUTION	421.1	@	[	]	%	$
CALM/LOG TRANSMISSION RECORD	421.2	@	[	]	%	$
CALM ERROR MESSAGES	421.3	@	[	]	%	$
FISCAL LOCK	421.4	@	[	]	%	$
INVOICE TRACKING	421.5	@	[	]	%	$
FUND DISTRIBUTION (TEMP TRANS	421.6	@	[	]	%	$
INVOICE DLN COUNTER	421.7	@	[	]	%	$
FISCAL STACKED DOCUMENTS	421.8	@	[	]	%	$
INVOICE PARTIAL COUNTER	421.9					
CALM/LOG TEMPLATE MAPS	422	@	[	]	%	$
COUNTER	422.2	@	[	]	%	$
CALM/LOG CODE SHEET	423	@	[	]	%	$
ISMS REASON CODES	423.4	@	@	^	^	^
PRC IFCAP MESSAGE ROUTER	423.5	@	[	]	%	$
ISMS/FMS TRANS	423.6	@	[	]	%	$
CALM/LOG BATCH TYPE	423.9	@	[	]	%	$
1358 DAILY RECORD	424	@	[	]	%	$
1358 AUTHORIZATION DETAIL	424.1	@	[	]	%	$

File Name	Number	DD Access	RD Access	WR Access	DEL Access	LAYGO Access
VENDOR	440	@	[	]	@	
DIRECT DELIVERY PATIENTS	440.2	@	[	]	#	
VENDOR EDIT	440.3					
PURCHASE CARD INFORMATION	440.5	@	@	@	@	@
PURCHASE CARD ORDER RECONCILE	440.6	@	@	@	@	@
MONTHLY ACCRUAL	440.7	@	@	@	@	@
PRCH AFC CHARGE TRANSMISSION	440.8	@	@	@	@	@
ITEM MASTER	441	@	[	]	#	$
FEDERAL SUPPLY CLASSIFICATION	441.2	@	@	@	@	@
FSC GROUP TITLES	441.3	@	@	@	@	@
DLA/LOG CODES	441.4	@	@	@	@	@
TYPE OF REQUISITION AMENDMENT	441.6					
AMENDMENTS TO DELIVERY SCHEDU	441.7					
PROCUREMENT & ACCOUNTING TRAN	442	@	[	]	%	$
TYPE OF AMENDMENT	442.2	@	@	@	@	@
PURCHASE ORDER STATUS	442.3	@	@	@	@	@
PURCHASE AUTHORITY	442.4	@	[	]	#	#
PAT TYPE	442.5	@	@	@	@	@
PAT NUMBER	442.6	@	[	]	%	
ADMINISTRATIVE CERTIFICATIONS	442.7	@	[	]	@	$
DELIVERY SCHEDULE (ORDER)	442.8					
ELEC RECEIVING REPORT BATCH	442.9	@	@	@	@	@
REQUEST WORKSHEET	443	@	@	@	@	@
IFCAP PURGEMASTER WORKLIST	443.1					
IFCAP PURGE PARAMETERS	443.2					
IFCAP PURGE INPROCESS	443.3					
TYPE OF SPECIAL HANDLING	443.4					
P.O./REQUEST/R.R. PRINT LOG	443.5	@	@	@	@	@
AMENDMENTS	443.6	@	@	@	@	@
EDI SENDER	443.75	@	@	@	@	@
EDI ERROR CODES	443.76	@	@	@	@	@
LOCAL PROCUREMENT REASON CODE	443.8	@	@	@	@	@
IFCAP PENDING ARCHIVE	443.9					
REQUEST FOR QUOTATION	444	@	[	]	%	$
RFQ VENDOR	444.1	@	[	]	%	$
SIC CODE	444.2	@	[	]	%	$
SIC CODE GROUPS	444.21	@	@	@	@	@
RFQ COUNTER	444.3	@	@	@	@	@
RFQ EDITING PREFERENCE	444.4	@	[	]	@	@
GENERIC INVENTORY	445	@		@	@	@
INVENTORY BALANCES	445.1	@		@	@	@
INVENTORY TRANSACTION	445.2	@		@	@	@
INTERNAL DISTRIBUTION ORDER/A	445.3	@		@	@	@
STORAGE LOCATION	445.4	@		@	@	@
GROUP CATEGORY	445.6	@		@	@	@
CASE CARTS	445.7	@		@	@	@
INSTRUMENT KITS	445.8	@		@	@	@
DISTRIBUTION/USAGE HISTORY	446	@		@	@	@
INVENTORY DISTRIBUTED PATIENT	446.1	@		@	@	@
BARCODE PROGRAM	446.4	@		@	@	@
CUSTOM LABEL	446.5	@		@	@	@
SPECIALTY COMMANDS	446.6	@		@	@	@
INVENTORY LOCK MANAGEMENT	447	@	@	@	@	@

(This page intentionally left blank.)